Oct. 3, 2016

Ms. Marlene H. Dortch, Secretary
Federal Communications Commission 445 12th St. SW
Washington, DC 20554

Re: Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106

Dear Ms. Dortch:

On Thursday, September 29, 2016, Brandi Collins and Anika Collier Navaroli of Color Of Change (COC) met with Gigi Sohn and Stephanie Weiner of the Chairman's Office and Daniel Kahn of the Wireline Bureau to discuss matters in the above referenced proceeding. During the meeting COC shared views on several aspects of the rulemaking including de-identification, the categorization of data as sensitive or non-sensitive, and pay-for-privacy models.

1. De-Identified Data

COC urged the FCC to reject any carve outs in the privacy rulemaking for de-identified data. The process of re-identification often occurs by combining data sets- one that typically contains anonymized or de-identified data and another that contains identifying information generally available to the public. To illustrate how easily data could be re-identified, computer science professor Latanya Sweeney conducted a study using census data, and found that zip code, birth date, and sex could be combined to identify 87% of the United States population.[1]

[1] Latanya Sweeney, k-anonymity: A Model for Protecting Privacy, International Journal on Uncertainty,

By the nature of the Black American experience, individuals belonging to that class tend to have extensive amounts of identifying data publicly available. This sheer volume of data creates even larger public databases from which seemingly anonymized data can be re-identified.

In additional to the vulnerability of re-identifying specific individuals, COC also cautioned against de-identified data being used to create a model of a larger group of alike individuals. Marketing and advertising schemes exist to target specific demographics based on assumptions made and collected about a larger group. In the digital context, the amount of de-identified data available to BIAS providers allows them to create models that lay the groundwork for predatory advertising and marketing.

2. Sensitive and Non-sensitive Data Distinction

COC reiterated our argument that opt-in notice and affirmative consent should be standard for all data, not just sensitive information. Here, the distinction between what is considered sensitive data and what is considered non-sensitive data is mostly left up to context. Information that for one group is considered innocuous can be considered sensitive to another group, particularly communities of color. For instance, an IP address can often be used to determine the location an internet user lives which in turn can correlate to race and income level.[2]

Relatedly, non-sensitive information can often be proxy for protected class information in our increasingly data centric world. Using the example of car insurance discounts, COC illustrated how Auto Insurance Telematics Devices collect what would be considered "non-sensitive" data- such as vehicle speed, the time of day someone is driving, the miles driven, and the rates of acceleration and braking. These devices do not collect "sensitive" data- such as location or the driver's identity.[3] By measuring non-sensitive data like the time of day a person is driving, car insurance companies can be engaged in pricing discrimination against individuals who work night shifts and tend to be of lower socioeconomic status and members of communities of color.[4] Thus, regardless of the distinction, information drawn from the non-sensitive data can easily become proxy for protected class and sensitive information.

---

[2] Alethea Lange & Rena Coen, *How Does the Internet Know Your Race?*, CENTER FOR DEMOCRACY & TECHNOLOGY (Sept. 7, 2016), https://cdt.org/blog/how-does-the-internet-know-your-race/.
[3] Peppet, Scott R., *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security & Consent* (March 1, 2014). Texas Law Review, Forthcoming. Available at SSRN:http://ssrn.com/abstract=2409074
[4] Saenz, Rogelio, *A Demographic Profile of U.S. Workers Around the Clock*, accessed online at http://www.prb.org/Publications/Articles/2008/workingaroundtheclock.aspx, on Sept. 29, 2016.

COC also urged that in making specific decisions as to what data should be deemed sensitive, the FCC confer with computer scientists and data experts to develop a list that would remain evergreen as technology and data analytics practices increasingly expand.

3. Pay-for-privacy Regimes

COC expressed its firm stance against any scheme that requires payment for data to be protected. These systems will inevitably create a two-tiered level of data privacy protection based on upon those who can afford to pay and leave behind those who cannot.

It has been estimated that these pay-for-privacy schemes could vary from $800 to $1000 per year.[5] With the median income of Black households in 2015 at $36,898,[6] the additional cost to protect privacy is too steep of a financial burden. Black people should not have to choose between broadband access and their right to data privacy.

COC also urged the FCC to be skeptical of any other financial incentives offered by companies to induce customers to make privacy choices. These incentives will begin the path to disparate impact on communities of color, as there is no proof that the promised savings will be passed along to consumers.

Respectfully submitted,

Brandi Collins
Director of Campaigns: Economic, Environmental & Media Justice Departments
1714 Franklin Street, #100-136
Oakland, CA 94612
510-663-4840 Ext 19

[5] *See, e.g.*, Karl Bode, *Think Tank Argues that Giving Up Privacy Is Good for the Poor*, Techdirt (Aug. 18, 2016), https://www.techdirt.com/articles/20160816/ 07164935254/think-tank-argues-that-giving-up-privacy-is-good-poor.shtml.
[6] Proctor, Bernadette D. and DeNavas-Walt, Carmen, *Income and Poverty in the United States: 2015*, https://www.census.gov/content/dam/Census/library/publications/2016/demo/p60-256.pdf